儿童手表安全性研究

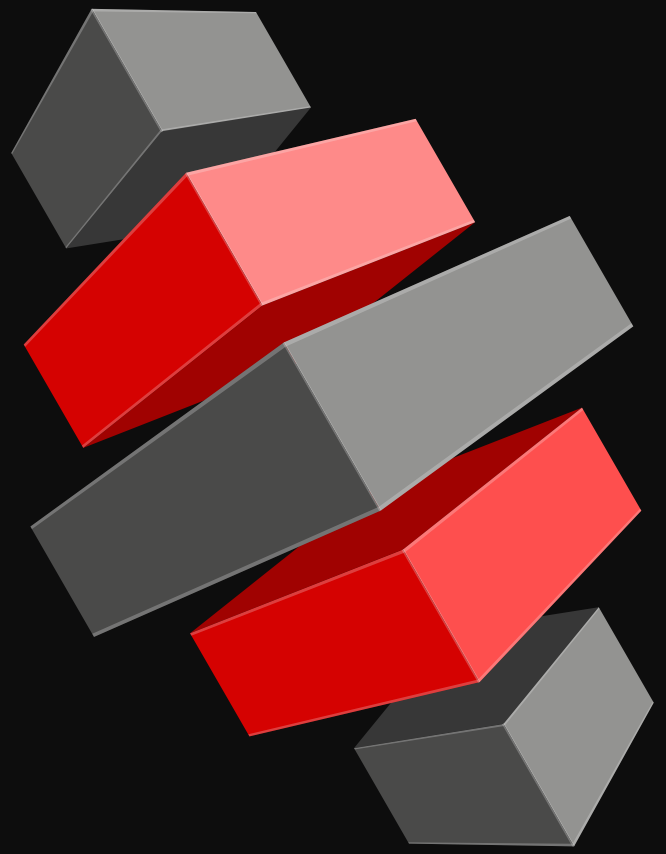
中北大学-刘波

稻壳儿 Docer

目录


1
绑定连接过程

绑定连接过程



- 将SIM卡放到手表内，开机，显示激活二维码
- 手机下载360儿童卫士，登录360账号
- 扫描二维码，输入手表SIM卡号
- 验证二维码，验证手机号
- 绑定成功


2
手表安全措施

手表安全措施

一键SOS
远程拍照

安全区域
运动轨迹

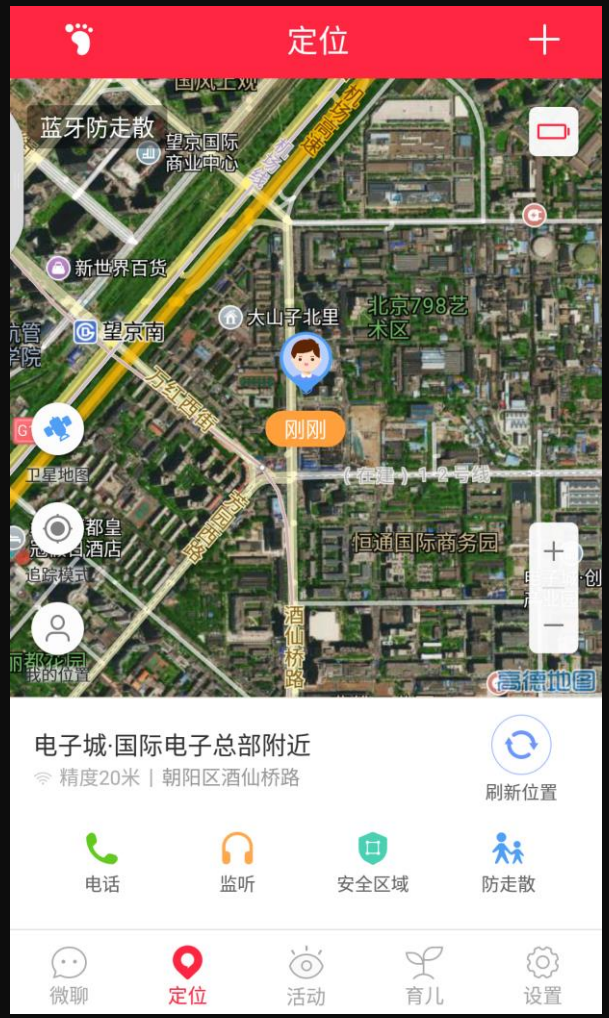
蓝牙防走散
数据安全

自动拦截陌生来电
位置信息双重加密

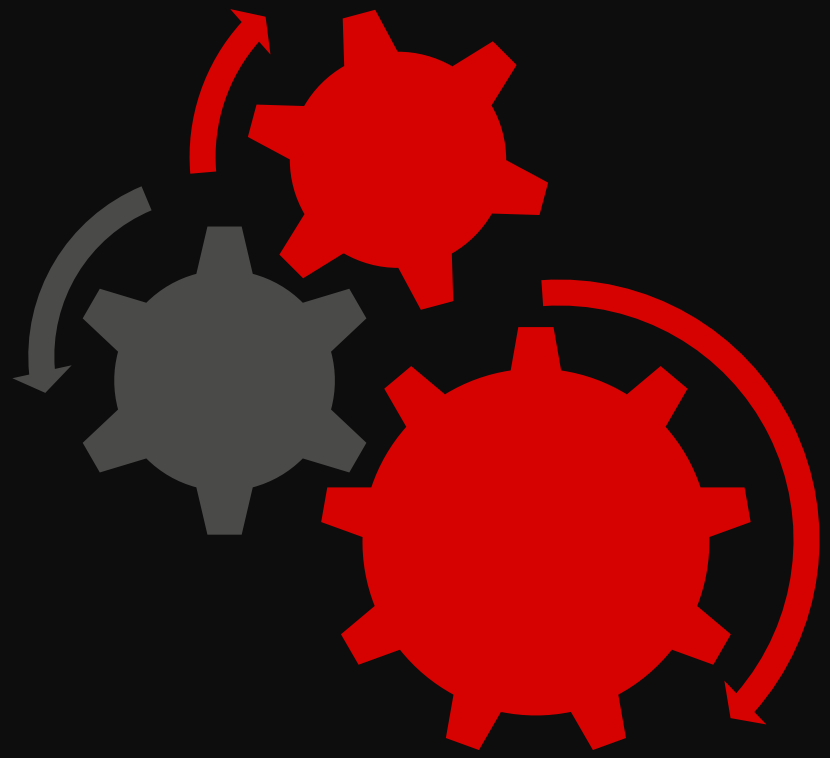
单向语音监听
服务端双向鉴权

攻击场景（二）


设置
宝贝
18265331182
健康计步
8558 步
闹钟
未设置
手表相册
手表通讯录
上课禁用
未设置
手表WiFi
未设置
省电时段
未开启
远程关机
微聊
定位
活动
育儿
设置


定位
蓝牙防走散
望京国际商业中心
新世界百货
望京南
大山子北里
北京798艺术区
刚刚
卫星地图
都皇酒店
恒通国际商务园
酒仙桥路
高德地图
电子城·国际电子总部附近
精度20米 | 朝阳区酒仙桥路
刷新位置
电话
监听
安全区域
防走散
微聊
定位
活动
育儿
设置

手表安全措施



通体只有一个按钮，激活后，不能主动关机，避免儿童误挤压关闭儿童手表导致的安全措施失效。

一直开启GPRS数据，时刻同服务端进行数据交换


3
可能的攻击面

可能的攻击面

使用移动联通卡
只支持2G

GSM

bluetooth 4.0
JUST WORK 模式

蓝牙

手表可以连接WIFI

WIFI

GPS定位

GPS

可能的攻击面

单击此处添加您的内容。

单击此处添加您的内容。

单击此处添加您的内容。

单击此处添加您的内容。

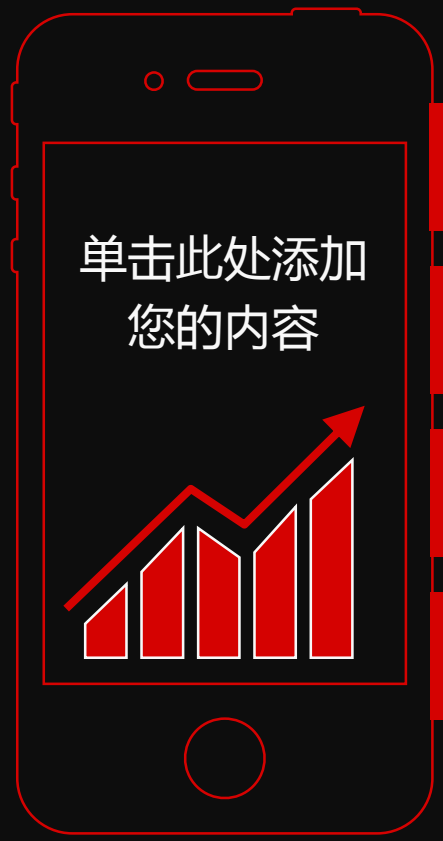
单击此处添加您的内容。

单击此处添加您的内容。

单击此处添加您的内容。

单击此处添加您的内容。

可能的攻击面



单击此处添加您的内容。 1

单击此处添加您的内容。 2

单击此处添加您的内容。建议您在展示时采用微软雅黑字体。 3

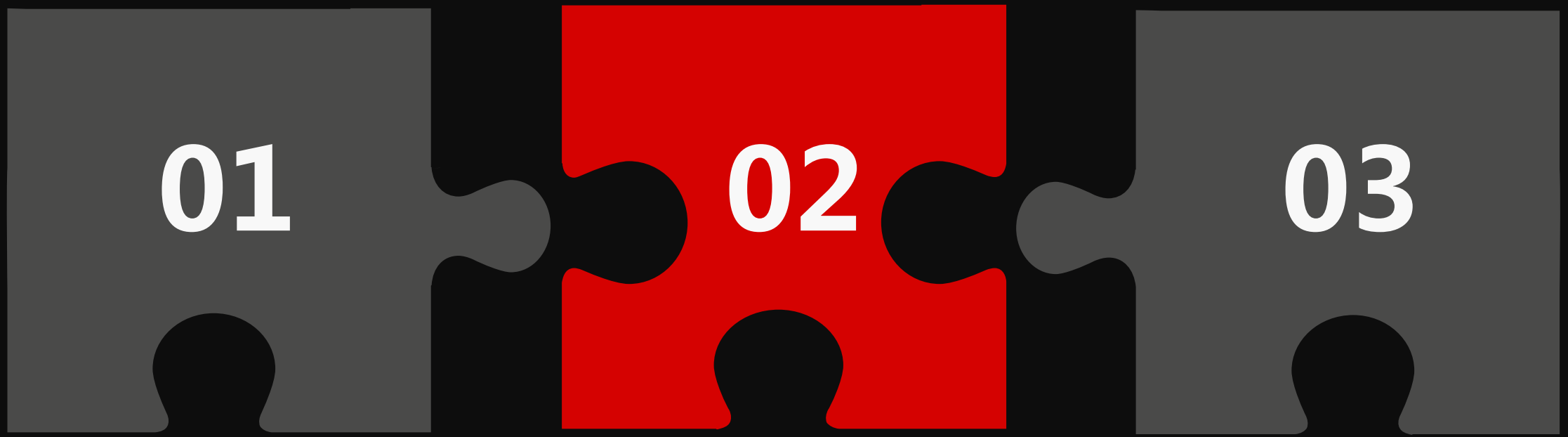
单击此处添加您的内容。建议您在展示时采用微软雅黑字体。 4

58%

单击此处添加您的内容。


4
两种攻击场景

攻击场景（一）



家长带领儿童去
客流量多的景区
或者顾客多的大型商场

架设无线电发射台，攻击
SOS、蓝牙防走散、语音监
听、远程拍照、定位等功能

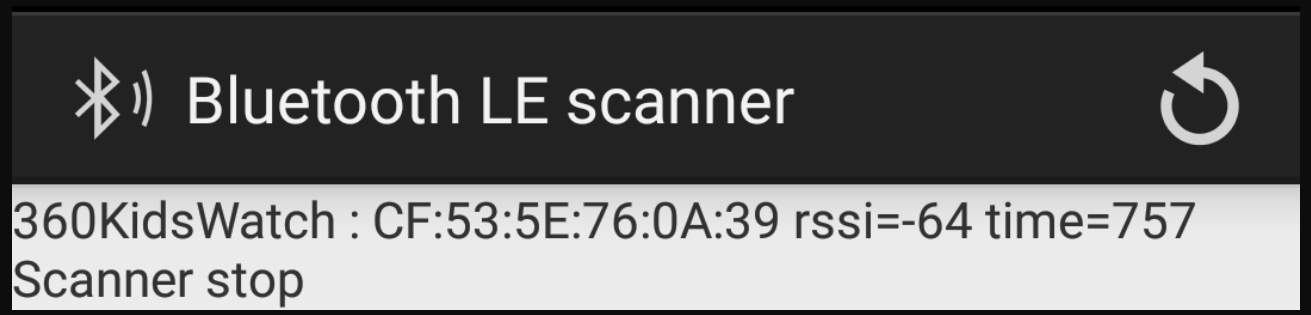
实施攻击
拐走儿童

攻击场景（一）

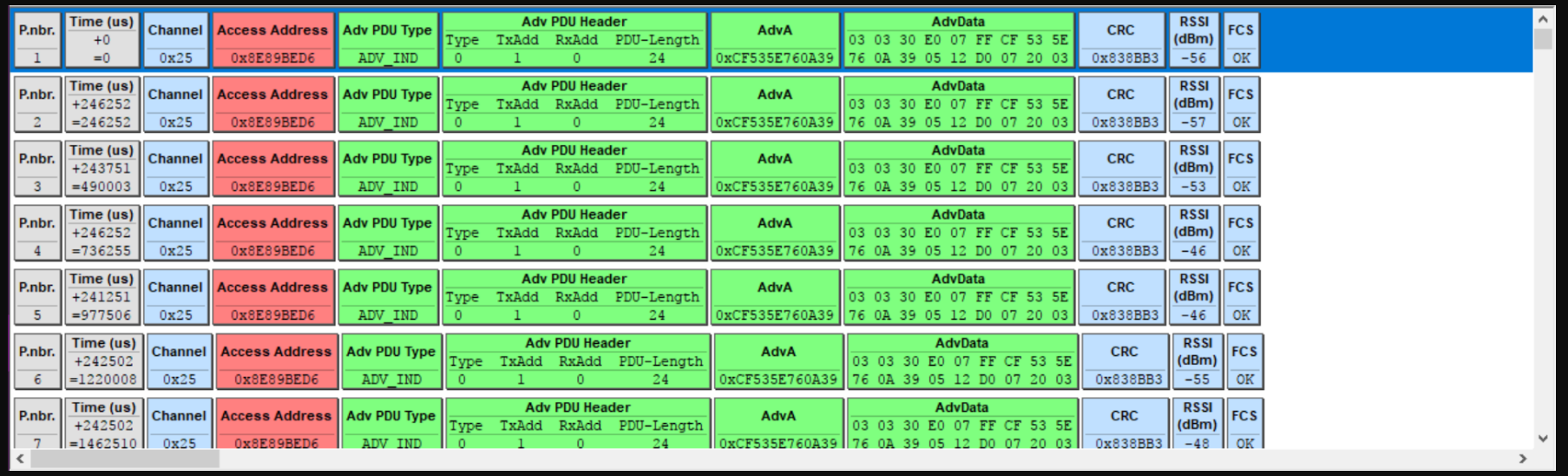

```
<string name="add_watch_error_49">手表正处于蓝牙防走散不能响应请求</string>
<string name="ble_close_hint">已关闭，手表蓝牙可到“我的-更多设置”中关闭。其他手表不变</string>
<string name="ble_open_hint">已开启，手表蓝牙也会被同步开启</string>
<string name="ble_tips_contents">蓝牙防走散在陌生区域中断会用红色警报提醒家长。在安全区域内断开则以较弱的橙色警报替代。为避免打扰，也可以关闭在安全区域
<string name="bt_close_monitor">已关闭蓝牙防走散</string>
<string name="bt_connect_monitor_success">已进入蓝牙防走散</string>
<string name="bt_connect_promot">当%1$s在您的身边时，手表将自动进入蓝牙防走散。 </string>
<string name="bt_connected_status_text">蓝牙防走散</string>
<string name="bt_desc">蓝牙4.0在低功耗状态下工作时，几乎不耗电，请放心使用。 </string>
<string name="bt_dont_support">您的手机不支持此功能（需手机支持蓝牙4.0且安卓版本在4.3及以上） </string>
<string name="bt_in_monitor">%1$s在当前位置处于蓝牙防走散</string>
<string name="bt_monitor_connected_with_me">我和%1$s处于蓝牙防走散</string>
<string name="bt_monitor_connected_with_other">%1$s和%2$s处于蓝牙防走散</string>
<string name="bt_monitor_opend_bt_dialog_content">蓝牙防走散下，将会开启并使用手机的蓝牙功能。 </string>
<string name="bt_monitor_opend_bt_dialog_content">蓝牙防走散下，将会开启并使用手机的蓝牙功能。 </string>
<string name="bt_monitor_opend_bt_dialog_title">开启蓝牙 </string>
<string name="bt_monitor_opend_net_dialog_content">蓝牙防走散下手表会依赖手机客户端定位并进入低功耗模式，为了能够正常定位，请确认手机处于联网状态。 <
<string name="bt_monitor_radio_title">蓝牙防走散</string>
<string name="bt_not_open">请先打开列表顶端的蓝牙开关</string>
<string name="bt_setting_close">手机蓝牙 ：已关闭</string>
<string name="bt_setting_close_bt">将关闭手机的蓝牙。 </string>
<string name="bt_setting_dlg_title_close_bt">关闭蓝牙 </string>
<string name="bt_setting_dlg_title_open_bt">开启蓝牙 </string>
<string name="bt_setting_open">手机蓝牙 ：已开启</string>
<string name="bt_setting_open_bt">将开启手机的蓝牙。 </string>
<string name="bt_setting_tips">开启后，宝贝在身边时将自动进入蓝牙防走散,需要手机和手表都打开蓝牙，手表离手机超出一定距离就会报警。建议外出旅行逛街时开启
<string name="bt_setting_tips">开启后，宝贝在身边时将自动进入蓝牙防走散,需要手机和手表都打开蓝牙 ，手表离手机超出一定距离就会报警。建议外出旅行逛街时开启
<string name="connected_monitor">%1$s已进入蓝牙防走散</string>
<string name="disconnected_monitor">%1$s已退出蓝牙防走散</string>
<string name="permission_location_bt_fail">获取定位权限失败，蓝牙防走散功能需要定位权限，请开启该权限</string>
<string name="setting_blue">蓝牙防走散</string>
<string name="settings_is_bt_dont_disturb_sub">安全区内断开蓝牙防走散时响橙色警报，关闭则不提醒</string>
<string name="settings_is_monitor">蓝牙防走散</string>
<string name="watch_setting_blue_close">已关闭，手表蓝牙需您手动关闭</string>
<string name="watch_setting_blue_open">已开启，手表蓝牙也会被同步开启</string>
<string name="watch_setting_blue_status">手表蓝牙状态</string>
<string name="watch_setting_blue_status_hint">“蓝牙防走散”功能须要手表蓝牙打开</string>
<string name="watch_setting_blue_status_hint">“蓝牙防走散”功能须要手表蓝牙打开</string>
```

攻击场景（二）

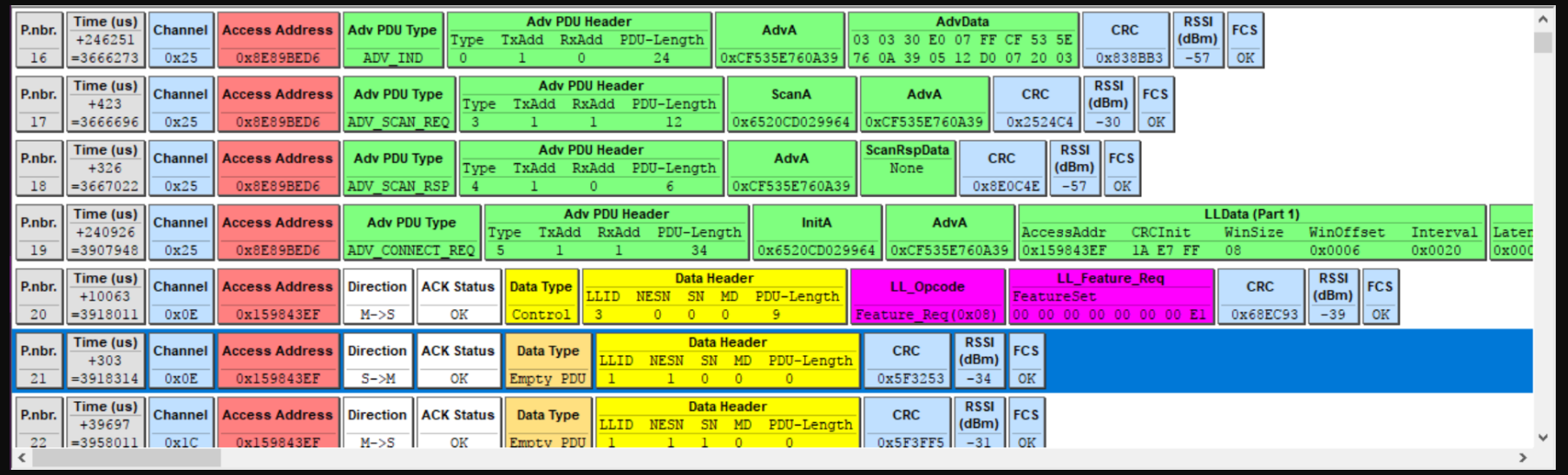

11:20
1.15K/s
4G
43%
蓝牙防走散
手机蓝牙
蓝牙4.0在低功耗状态下工作时，几乎不耗电，请放心使用。
走失提醒
酒仙桥路7号院
电子城·国际
360大厦
您的孩子已走开一定距离，请立即确认宝贝当前状况是否安全！
关闭
查看
开启后，宝贝在身边时将自动进入蓝牙防走散,需要手机和手表都打开蓝牙，手表离手机超出一定距离就会报警。建议外出旅行逛街时开启。


Bluetooth LE scanner
360KidsWatch : CF:53:5E:76:0A:39 rssi=-64 time=757
Scanner stop

攻击场景（一）



P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	AdvData	CRC	RSSI (dBm)	FCS
					Type TxAdd RxAdd PDU-Length					
1	+0 =0	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-56	OK
2	+246252 =246252	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-57	OK
3	+243751 =490003	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-53	OK
4	+246252 =736255	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-46	OK
5	+241251 =977506	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-46	OK
6	+242502 =1220008	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-55	OK
7	+242502 =1462510	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-48	OK



P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	AdvData	CRC	RSSI (dBm)	FCS
					Type TxAdd RxAdd PDU-Length					
16	+246251 =3666273	0x25	0x8E89BED6	ADV_IND	0 1 0 24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-57	OK

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	ScanA	AdvA	CRC	RSSI (dBm)	FCS
					Type TxAdd RxAdd PDU-Length					
17	+423 =3666696	0x25	0x8E89BED6	ADV_SCAN_REQ	3 1 1 12	0x6520CD029964	0xCF535E760A39	0x2524C4	-30	OK

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	ScanRspData	CRC	RSSI (dBm)	FCS
					Type TxAdd RxAdd PDU-Length					
18	+326 =3667022	0x25	0x8E89BED6	ADV_SCAN_RSP	4 1 0 6	0xCF535E760A39	None	0x8E0C4E	-57	OK

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header	InitA	AdvA	LLData (Part 1)					
					Type TxAdd RxAdd PDU-Length			AccessAddr	CRCInit	WinSize	WinOffset	Interval	Later
19	+240926 =3907948	0x25	0x8E89BED6	ADV_CONNECT_REQ	5 1 1 34	0x6520CD029964	0xCF535E760A39	0x159843EF	1A E7 FF	08	0x0006	0x0020	0x000

P.nbr.	Time (us)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header	LL_Opcode	LL_Feature_Req	CRC	RSSI (dBm)	FCS
							LLID NESN SN MD PDU-Length		FeatureSet			
20	+10063 =3918011	0x0E	0x159843EF	M->S	OK	Control	3 0 0 0 9	Feature_Req(0x08)	00 00 00 00 00 00 00 E1	0x68EC93	-39	OK

P.nbr.	Time (us)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header	CRC	RSSI (dBm)	FCS
							LLID NESN SN MD PDU-Length			
21	+303 =3918314	0x0E	0x159843EF	S->M	OK	Empty PDU	1 1 0 0 0	0x5F3253	-34	OK

P.nbr.	Time (us)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header	CRC	RSSI (dBm)	FCS
							LLID NESN SN MD PDU-Length			
22	+39697 =3958011	0x1C	0x159843EF	M->S	OK	Empty PDU	1 1 1 0 0	0x5F3FF5	-31	OK

攻击场景（一）

P.nbr.	Time (us)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header					CRC	RSSI (dBm)	FCS
							LLID	NESN	SN	MD	PDU-Length			
186	+39769 =4763013	0x1E	0x159843EF	M->S	OK	Empty PDU	1	0	0	0	0	0x5F3480	-32	OK
187	+231 =4763244	0x1E	0x159843EF	S->M	OK	Empty PDU	1	1	0	0	0	0x5F3253	-39	OK
188	+39769 =4803013	0x07	0x159843EF	M->S	OK	Empty PDU	1	1	1	0	0	0x5F3FF5	-40	OK
189	+231 =4803244	0x07	0x159843EF	S->M	OK	Empty PDU	1	0	1	0	0	0x5F3926	-36	OK
190	+39770 =4843014	0x15	0x159843EF	M->S	OK	Empty PDU	1	0	0	0	0	0x5F3480	-31	OK
191	+230 =4843244	0x15	0x159843EF	S->M	OK	Empty PDU	1	1	0	0	0	0x5F3253	-42	OK
192	+39770 =4883014	0x23	0x159843EF	M->S	OK	Empty PDU	1	1	1	0	0	0x5F3FF5	-36	OK

P.nbr.	Time (us)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header					CRC	RSSI (dBm)	FCS
							LLID	NESN	SN	MD	PDU-Length			
939	+39771 =20603084	0x18	0x159843EF	M->S	OK	Empty PDU	1	0	0	0	0	0x5F3480	-30	OK
940	+231 =20603315	0x18	0x159843EF	S->M	OK	Empty PDU	1	1	0	0	0	0x5B3253	-78	FCE ERROR
941	+39770 =20643085	0x01	0x159843EF	M->S	OK	Empty PDU	1	1	1	0	0	0x5F3FF5	-35	OK
942	+40000 =20683085	0x0F	0x159843EF	M->S	RETRY	Empty PDU	1	1	1	0	0	0x5F3FF5	-36	OK
943	+40001 =20723086	0x1D	0x159843EF	M->S	RETRY	Empty PDU	1	1	1	0	0	0x5F3FF5	-40	OK
944	+40002 =20763088	0x06	0x159843EF	M->S	RETRY	Empty PDU	1	1	1	0	0	0x5F3FF5	-52	OK
945	+40000 =20803088	0x14	0x159843EF	M->S	RETRY	Empty PDU	1	1	1	0	0	0x5F3FF5	-48	OK

攻击场景（一）

P.nbr.	Time (us)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header					CRC	RSSI (dBm)	FCS
							LLID	NESN	SN	MD	PDU-Length			
1032	+40001 =24083160	0x15	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-34	OK
1033	+40001 =24123161	0x23	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-33	OK
1034	+40001 =24163162	0x0C	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-34	OK
1035	+40001 =24203163	0x1A	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-30	OK
1036	+40000 =24243163	0x03	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-36	OK
1037	+40002 =24283165	0x11	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-34	OK
1038	+40000 =24323165	0x1F	0x159843EF	M->S	RETRY	Empty PDU	1	0	0	0	0	0x5F3480	-31	OK

攻击场景（一）

OpenBTS

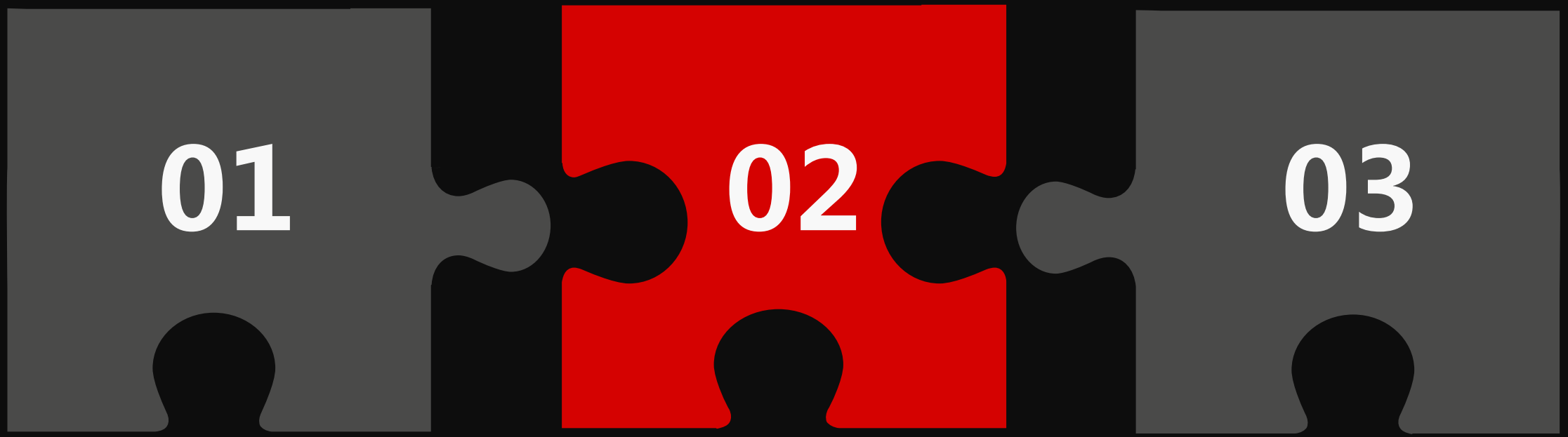
通过把手表的通信全部定向到伪基站，来攻击手表的SOS、蓝牙防走散、语音监听、远程拍照、定位等功能

攻击场景（一）

GPS-SIM

通过欺骗手表的GPS，攻击手表的安全区域等功能。

攻击场景（二）



儿童带着手表在幼儿园的活动场所玩耍

连接手表蓝牙，获取手表内信息，如家长电话号码

实施社会工程学攻击进行诈骗和勒索

攻击场景（二）

P.nbr.	Time (us)	Channel	Access Address	Adv PDU Type	Adv PDU Header				AdvA	AdvData	CRC	RSSI (dBm)	FCS
					Type	TxAdd	RxAdd	PDU-Length					
1	+0 =0	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-56	OK
2	+246252 =246252	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-57	OK
3	+243751 =490003	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-53	OK
4	+246252 =736255	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-46	OK
5	+241251 =977506	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-46	OK
6	+242502 =1220008	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-55	OK
7	+242502 =1462510	0x25	0x8E89BED6	ADV_IND	0	1	0	24	0xCF535E760A39	03 03 30 E0 07 FF CF 53 5E 76 0A 39 05 12 D0 07 20 03	0x838BB3	-48	OK

攻击场景（二）

蓝牙4.0的几种配对方式

Numeric Comparison：配对双方都显示一个6位的数字，由用户来核对数字是否一致，一致即可配对。例如手机之间的配对。

Just Works：用于配对没有显示没有输入的设备，主动发起连接即可配对，用户看不到配对过程。例如连接蓝牙耳机。

Passkey Entry：要求配对目标输入一个在本地设备上显示的6位数字，输入正确即可配对。例如连接蓝牙键盘。

Out of Band：两设备的通过别的途径交换配对信息，例如NFC等。例如一些NFC蓝牙音箱。

攻击场景（二）

Classic中这四个配对方式就是SSP简单配对中四种模式。蓝牙配对流程主要防止两种攻击，MITM中间人攻击以及passive eavesdropping被动监听攻击。这四种配对方式，除开JUSTWORK外，都可以防止这两种攻击。JUSTWORK由于不涉及人机交互，所以没法防止MITM的中间人攻击。（插一句，传统蓝牙的PIN CODE配对方式就是由于无法防止被动监听攻击（穷举PIN码）才衍生了这四种SSP简单配对方式。）

2. BLE中LE配对分为4.0版本中的LE LEGACY配对方式以及在BLE4.2版本开始导入的BLE Secure Connection配对方式。
前者LEGACY中，配对方式三种，JUSTWORK，PASSKEY ENTRY，以及OOB，JUSTWORK依然无法防止MITM，另外由于秘钥生成方式的缺陷，导致LE LEGACY配对方式无法防止被动监听攻击（OOB可以防止，因为用了非空中的传输交互）
正因为此，BLE4.2版本把Secure connection也引入到了BLE中（为什么说也，是因为CLASSIC模式中也有SECURE CONNECTION方式...），
BLE Secure connection和CLASSIC 的SSP采用同样的ECDH加密方式，所以安全性恢复到同样等级，可以防止被动监听攻击了。BLE SECURE CONNECTION配对又有了四种配对模式，JUSTWORK，PASSKEY ENTRY，NUMERIC COMP.，以及OOB，同样类同于SSP，JUSTWORK防止不了MITM。

谢谢

THANK YOU FOR YOUR LISTENING

中北大学-刘波

稻壳儿 Docer